

# Security Predictions for 2012

## from Websense® Security Labs™

From SCADA to Sony, RSA, Comodo, and Diginotar, to hacktivism and WikiLeaks, 2011 was arguably the most unusual and unexpected year in the history of IT security. So what does 2012 have in store for us?

With an influx of bring your own devices (BYOD) and mobility, social media exploding, cloud computing knocking, and other operational challenges thrown in for good measure, if 2011 was the shocker, then 2012 is likely to be the kitchen sink of security concerns.

We got the Websense® Security Labs™ researchers together to brainstorm, whiteboard, and vote. The result is our list of events likely to be among those that drive your life—and ours—in 2012.

**1. Your social media identity may prove more valuable to cybercriminals than your credit cards. Bad guys will actively buy and sell social media credentials in online forums.** Spammers have been buying parcels of email credentials for a couple years now. We've seen carder sites where criminals can buy and sell your credit card information for pennies on the dollar. Want a South African issued card with a \$25,000 limit with the user's PIN? How about one from the U.S. issued by a bank in the Northeast along with the user's social security number? Old news. **Today, your social identity may have greater value to the bad guys.** Facebook has more than 800 million active users, and over half of them log on daily and they have an average of 130 friends. Trust is the basis of social networking, so if a bad guy compromises your social media log-ins, there is a good chance they can manipulate your friends. Which leads us to prediction #2.

**2. The primary blended attack method used in the most advanced attacks will be to go through your social media "friends," mobile devices and through the cloud.** Blended attacks used to be predominately about the use of email and web together. Many of the recent so-called advanced persistent threats (APTs) were simply email phishing scams. In 2012, **advanced attacks are going to increasingly use at least two, and sometimes all, of the following emerging technologies: social media, cloud platforms, and mobile.** We've

already seen one APT attack that used the chat functionality of a compromised social network account to get to the right user. Expect this to be the primary vector in the most persistent and advanced attacks of 2012.

**3. 1,000+ different mobile device attacks coming to a smartphone or tablet near you.** People have been predicting this for years, but in 2011 it actually started to happen. Expect more increases in exposed vulnerabilities from black hats and white hats in the coming year for mobile devices. In 2012, we estimate that you'll see more than 1,000 different variants of exploits, malicious applications, and botnets infecting that device glued to your hand and plugged into your head. We'll at least see a new variant every, day. Indeed, if application creators don't protectively sandbox their apps, we're also likely to see versions of malware that access your banking and social credentials as well as other sensitive data on your phone. This includes your work documents and any cloud applications you may have on that handy device. We'll also start seeing significantly more social engineering designed to specifically lure mobile users to infected apps and websites. And watch out: the number of people who fall victim to believable social engineering scams will go through the roof if the bad guys find a way to use mobile location-based services to design hyper-specific geolocation social engineering attempts.

4. **SSL/TLS will put net traffic into a corporate IT blind spot.** Two items are increasing traffic over SSL/TLS secure tunnels for privacy and protection. First, the disruptive growth of mobile and tablet devices are moving packaged software to the cloud and distributing data to new locations. Second, many of the largest, most commonly used websites, like Google search, Facebook, and Twitter have switched their sites to default to https sessions. You'd think this would just be a positive, since it encrypts the communications between the computer and destination. But as more traffic moves through encrypted tunnels, many traditional enterprise security defenses (like firewalls, IDS/IDP, network AV, and passive monitoring) are going to be left looking for a threat needle in a haystack, since they cannot inspect the encoded traffic. These blind spots provide a big doorway for cybercriminals to walk through.
5. **Containment is the new prevention.** For years, security defenses have focused on keeping cybercrime and malware out. There's been much less attention on watching outbound traffic for data theft and evasive command and control communications. But multiple studies show that the majority of data theft is related to hacking and malware. Websense Security Labs research estimates that more than 50 percent of data loss incidents happen over the web. DLP deployments have been delayed because of traditional long-winded, overwrought, and extensive data discovery projects. In 2012, organizations will look to stop data theft at corporate gateways that detect custom encryption, geolocations for web destinations, and command and control communications. **Organizations on the leading edge will implement outbound inspection and will focus on adapting prevention technologies to be more about containment, severing communications, and data loss mitigation after an initial infection.**
6. **The London Olympics, U.S. presidential elections, Mayan calendar, and apocalyptic predictions will lead to broad attacks by criminals.** SEO poisoning has become an everyday occurrence. You name the trend—it's going to be poisoned. Websense Security Labs still sees highly popular search terms deliver a quarter of the first page of results as poisoned. As the bigger search engines have become more savvy on removing poisoned results, **criminals in 2012 will use the same techniques ported to new platforms.** They will continue to take advantage of today's 24-hour, up-to-the minute news cycle, only now they will infect users where they are less suspicious: Twitter feeds, Facebook posts/emails, LinkedIn updates, YouTube video comments, and forum conversations. We recommend extreme caution with searches, wall posts, forum discussions, and tweets dealing with the topics listed above, as well as any celebrity death or other surprising news from the U.S. presidential campaign.
7. **Social engineering and rogue anti-virus will continue to reign.** Scareware tactics and the use of rogue anti-virus, which decreased a bit in 2011, will stage a comeback. When you combine how easy it is to acquire a malicious tool kit with the prevalence of the tools, which are designed to cause massive exploitation and compromise of websites, the result is resurgence in this type of crimeware. Except, instead of seeing "You have been infected" pages, **we anticipate three areas will emerge as growing scareware subcategories in 2012: a growth in fake registry clean-up, fake speed improvement software, and fake back-up software mimicking popular personal cloud backup systems.** Also expect that the use of polymorphic code and IP lookup will continue to be built into each of these tactics to bypass blacklisting and hashing detection by security vendors.